Milbank

December 4, 2014

CONTACTS

Richard Sharp
Partner
+1-212-530-5209
rsharp@milbank.com

Wayne M. Aaron
Partner
+1-212-530-5284
waaron@milbank.com

John M. Yarwood
Associate
+1-212-530-5369
jyarwood@milbank.com

Sagiv Edelman
Associate
+1-212-530-5310
sagivedelman@milbank.com

Financial Institutions Regulation Group Client Alert:

SEC Adopts Regulation SCI to Strengthen Controls for Technological Systems at Core of U.S. Markets

I. INTRODUCTION

On November 19, 2014, the SEC announced the adoption of Regulation Systems Compliance and Integrity ("Reg SCI") in a 742-page release.[1] Reg SCI is effective 60 days after publication in the Federal Register, and subject entities must comply with Reg SCI's requirements within nine months of that date.[2] Once effective, Reg SCI will regulate approximately 44 entities, including securities exchanges and certain alternative trading systems ("ATSs"). While broker-dealer-operated ATSs meeting certain trading volume minimums are covered by the new rules, the SEC notably *declined to extend* Reg SCI *to broker-dealers, generally*. Reg SCI imposes rigorous standards for subject entities' technological systems and related policies and procedures. The regulation also includes extensive reporting requirements. Concurrent with the adoption of Reg SCI, the SEC staff also issued guidance relating to the policies and procedures subject entities should adopt. The following discussion addresses Reg SCI's key provisions related to its applicability and requirements and identifies issues raised by its provisions.

II. ADOPTING RELEASE

The SEC initially proposed Reg SCI on March 13, 2013 in response to perceived vulnerabilities in the nation's securities market structure, including those related to

[1] *See Regulation Systems Compliance and Integrity*, Securities Exchange Act Release No. 34-73639 (Nov. 19, 2014) (to be codified at 17 C.F.R. §§ 242.1000-1007) (hereinafter, the "Adopting Release").

[2] *See* Adopting Release at 444. As of the publication of this article, the Adopting Release has not yet been published in the Federal Register.

recent incidents such as the BATS IPO, the Facebook IPO, and Knight Capital's technology issue.[3] The final rule largely tracks the initial proposal, with certain variations. Most notably, two key differences between the proposed regulation and Reg SCI as adopted are: (i) that the standards that subject entities must adhere to (discussed below) are no longer required to be widely available *for free*, but rather need only be widely available; and (ii) that the SEC will no longer require access to subject entities' systems, but will rely instead on required recordkeeping as a monitoring tool.

Reg SCI supersedes and replaces the SEC's current Automation Review Policy ("ARP")[4] and the segments of those policy statements that were later codified in Rule 301(b)(6) of the Securities Exchange Act of 1934 ("Exchange Act"), which applies to significant-volume ATSs that trade NMS and non-NMS stocks.[5] As discussed in more depth below, Reg SCI requires self-regulatory organizations, certain ATSs, plan processors, and certain clearing agencies to: (i) establish and maintain policies and procedures related to their technological systems; and (ii) provide certain notices and reports to the SEC.

III. APPLICABILITY

Reg SCI regulates any entity falling within the definition of an "SCI entity" defined as an "SCI self-regulatory organization, SCI alternative trading system, plan processor, or exempt clearing agency subject to ARP."[6] The SEC intends this definition to cover those entities that play a significant role in the U.S. securities markets and/or have the potential to impact investors, the overall market, or the trading of individual securities.[7] Reg SCI does not, however, cover OTC market makers, exchange market makers, order-entry firms, clearing broker-dealers or large multi-service broker-dealers. The regulation governs activity associated with the technological systems of SCI entities that are related to securities market activity.

A. SCI SRO

An SCI Self-Regulatory Organization ("SCI SRO") is any entity that is a national securities exchange registered under Section 6(b) of the Exchange Act, a registered

---

[3] *See* Securities Exchange Act Release No. 69077 (March 8, 2013), 78 Fed. Reg. 18084 (March 25, 2013) (hereinafter, the "Proposing Release").

[4] The ARP was established by the SEC's two policy statements, each titled "Automated Systems of Self-Regulatory Organizations," issued in 1989 and 1991. *See* Securities Exchange Act Release Nos. 27445 (November 16, 1989), 54 FR 48703 (November 24, 1989) and 29185 (May 9, 1991), 56 FR 22490 (May 15, 1991).

[5] 17 C.F.R. § 242.301(b)(6). *See also* Securities Exchange Act Release No. 40760 (December 8, 1998), 63 FR 70844 (December 22, 1998).

[6] Rule 1000.

[7] *See* Adopting Release at 27.

securities association, a registered clearing agency, or the Municipal Securities Rulemaking Board. There are two notable exceptions: (1) exchanges that list or trade security futures products that are registered with the SEC as a national securities exchange pursuant to Section 6(g) of the Exchange Act, and (2) any limited purpose national securities association registered with the SEC pursuant to Exchange Act Section 15A(k).[8]

B. SCI ATS

An SCI alternative trading system ("SCI ATS") is any ATS that, during at least four of the preceding six calendar months:

- Had 5% or more in any single NMS stock's average daily dollar volume ("ADDV") reported by applicable transaction reporting plans, and 0.25% or more in all NMS stocks' ADDV;
- Had one percent (1%) or more in all NMS stocks' ADDV; or
- Had with respect to equity securities that are not NMS stocks and for which transactions are reported to a self-regulatory organization, 5% or more of the ADDV as calculated by the self-regulatory organization to which such transactions are reported.[9]

Consequentially, entities that operate an ATS should closely monitor their trading volume.

The SEC believes that 12 unnamed entities currently fall within the definition of an SCI ATS.[10] Any ATS that meets the SCI ATS thresholds, subsequent to the initial compliance date, has six months to comply with Reg SCI.[11]

C. SCI Plan Processor

A Reg SCI Plan Processor is any entity that meets the definition in Rule 600(b)(55) of Regulation NMS, which defines "plan processor" as "any self-regulatory organization or securities information processor acting as an exclusive processor in connection with the development, implementation and/or operation of any facility contemplated by an effective national market system plan."[12]

---

[8] *See id.* at 33-34. Entities excepted from the definition of an SCI SRO are the National Futures Association and securities futures exchanges. *See id.* at 33 n.78.

[9] *See id.* at 39, 54-57, 66-67; Rule 1000.

[10] Based on data collected from ATSs pursuant to FINRA Rule 4552 for 18 weeks of trading in 2014. *See id.* at 55.

[11] *See id.* at 39.

[12] The definition includes processors of the CTA Plan, CQS Plan, Nasdaq UTP Plan, and OPRA Plan. *See id.* at 73 n.196.

D. Exempt Clearing Agencies

Reg SCI also applies to exempt clearing agencies previously subject to ARP pursuant to Section 17A of the Exchange Act or any SEC regulation that supersedes or replaces such policies.[13] An exempt clearing agency previously subject to ARP is defined as "an entity that has received from the [SEC] an exemption from registration as a clearing agency under Section 17A of the [Exchange] Act, and whose exemption contains conditions that relate to the [SEC's] [ARP], or any [SEC] regulation that supersedes or replaces such policies."[14]

E. Subject Systems of SCI Entities

Reg SCI applies to the specific systems of an SCI entity that directly support the six areas that the SEC has determined to have traditionally been central to the functioning of the U.S. securities markets, namely: (i) trading; (ii) clearance and settlement; (iii) order routing; (iv) market data; (v) market regulation; and (vi) market surveillance.[15] SCI systems include all computer, network, electronic, technical, automated, or similar systems of, or operated by or on behalf of, an SCI entity that, with respect to securities, directly support each of those areas. Any such systems are subject to all of the provisions of Reg SCI except for those systems that are "critical SCI systems."[16] As noted below, critical SCI systems are held to higher standards regarding certain Reg SCI requirements.

"Critical SCI systems" directly support functionality related to: (i) clearance and settlement systems of clearing agencies; (ii) openings, re-openings, and closings on primary trading markets; (iii) trading halts; (iv) initial public offerings; (v) the provision of consolidated market data (i.e., SIPs); or (vi) exclusively listed securities. Critical SCI systems also include those systems that provide functionality to the securities markets for which the availability of alternatives is significantly limited or nonexistent and without which there would be a material impact on fair and orderly markets.[17] Additionally, "indirect SCI systems" are only subject to the provisions relating to security and intrusions. Indirect SCI systems are only those

---

[13] *E.g.*, Omgeo Matching Services - US, LLC.

[14] Rule 1000.

[15] The SEC has limited SCI systems to include only those systems relating to market regulation and market surveillance rather than all regulation and surveillance systems (*e.g.*, systems relating to dispute resolution or capital requirements). *See* Adopting Release at 89.

[16] *See id.* at 79.

[17] This last prong of the definition is a "catch-all provision" designed to account for further technology advancements and the continual evolution of the securities markets. The SEC stated that it was not aware of any SCI systems that would satisfy this prong of the definition at the time of the publication of the Adopting Release. *See id.* at 105-06.

that are operated by or on behalf of an SCI entity that, if breached, would be reasonably likely to pose a security threat to SCI systems.[18]

IV. SCI EVENTS

Reg SCI identifies and prescribes specific requirements related to three defined "SCI events": systems disruptions, systems compliance issues, and systems intrusions. In the Proposing Release, the SEC listed certain events as examples of systems disruptions, including: (i) a failure to maintain service-level agreements; (ii) a disruption of normal operations; (iii) a loss of use of any SCI system; (iv) a loss of transaction or clearance and settlement data; (v) significant delays in processing; (vi) a significant diminution of ability to disseminate timely and accurate market data; or (vii) a queuing of data of such duration that normal service delivery is affected.[19] The SEC removed these seven specific criteria in the adopted regulation because it believed that the proposed definition was both under-inclusive and over-inclusive.[20] Instead, a systems disruption is defined as an event in an SCI entity's SCI systems that disrupts, or significantly degrades, the normal operation of an SCI system.[21] A systems compliance issue is "an event at an SCI entity that has caused any SCI system of such entity to operate in a manner that does not comply with the [Exchange] Act and rules and regulations thereunder or the entity's rules or governing documents, as applicable." Significantly, there is no materiality threshold for either a systems disruption or a systems compliance issue.

A systems intrusion is any unauthorized entry into any SCI system or indirect SCI system of an SCI entity. The SEC intends, with this definition, to cover any unauthorized entry into SCI systems or indirect SCI systems, regardless of the identity of the person committing the intrusion (whether outsiders, employees, or agents of the SCI entity), and regardless of whether or not the intrusion was part of a cyber attack, potential criminal activity, or other unauthorized attempt to retrieve, manipulate, or destroy data, or access or disrupt systems of SCI entities.[22] The

---

[18] The definition of "indirect SCI systems" does not include any systems of an SCI entity for which the SCI entity establishes reasonably designed and effective controls that result in SCI systems being logically or physically separated from such non-SCI systems. *See id.* at 111. References to "indirect SCI systems" are included in the definitions of "responsible SCI personnel," "SCI review," and "systems intrusion" in adopted Rule 1000. Rule 1001(a), requiring reasonably designed policies and procedures to ensure operational capability, applies to indirect SCI systems only for purposes of security standards. In addition, Rule 1002, which relates to an SCI entity's obligations with regard to SCI events, applies to indirect SCI systems only with respect to systems intrusions. Further, pursuant to Rule 1003(a), the obligations related to systems changes apply to material changes to the security of indirect SCI systems. In addition, the requirements regarding an SCI review apply to indirect SCI systems. *See id.* at 113-14.

[19] *See id.* at 124-25.

[20] *See id.* at 125.

[21] A system is disrupted when its normal operation is halted. A system is degraded when its performance and functionality suffers (*e.g.*, data queuing or slowing of response times). *See id.* at 125, 126 n.384.

[22] See *id.* at 140-41.

definition does not include unsuccessful attempts at unauthorized entry. There is also no materiality threshold for a systems intrusion. Given the definition's unqualified inclusion of any unauthorized access by any person, potential SCI entities should establish comprehensive and effective monitoring policies and procedures related to SCI systems in order to detect and investigate potentially unauthorized access of those systems. These policies and procedures should account for not only attacks and intrusions by outsiders, but also access of SCI systems by unauthorized employees. Further, SCI entities should develop comprehensive training programs related to SCI-systems access for both authorized and unauthorized employees.

V. SCI ENTITY OBLIGATIONS

Reg SCI requires subject entities to adopt and implement policies and procedures related to their technological systems, take corrective actions whenever an SCI event occurs, report to the SEC certain information related to its systems and SCI events, and maintain and keep certain records. These requirements raise certain operational, compliance, and litigation-related issues.

A. Policies and Procedures

Each SCI entity must establish, maintain, and enforce written policies and procedures reasonably designed to ensure that its SCI systems and -- for purposes of security standards, indirect SCI systems -- have levels of capacity, integrity, resiliency, availability, and security, adequate to maintain the SCI entity's operational capability and promote the maintenance of fair and orderly markets.[23] An SCI entity must also establish, maintain, and enforce written policies and procedures reasonably designed to ensure that its SCI systems operate in a manner that complies with the Exchange Act and the rules and regulations thereunder and the entity's rules and governing documents, as applicable. This means that SCI SROs and ATSs will not only be subject to securities laws, regulations and rules, but also are required to comply with their own rules and standards related to systems, such as ATS-member handbooks. These requirements are necessarily flexible to account for the nature of each SCI entity's business, technology and practices. These policies and procedures should include:

(i) current and future capacity planning estimates;

(ii) periodic capacity stress tests of systems;

[23] *See* Rule 1001(a).

(iii) a program to review and keep systems development and testing methodology current;[24]

(iv) regular reviews and testing of SCI systems, including backup systems, to identify vulnerabilities pertaining to internal and external threats, physical hazards, and natural or man-made disasters;

(v) business continuity and disaster recovery plans that are sufficiently resilient and geographically diverse to ensure next business day resumption of trading and two-hour resumption of clearance and settlement services following a wide-scale disruption;[25]

(vi) standards that result in systems being designed, developed, tested, maintained, operated, and monitored in a manner that facilitates the successful collection, processing, and dissemination of market data;

(vii) monitoring of such systems to identify potential SCI events;

(viii) testing of all SCI systems and any changes to SCI systems prior to implementation;

(ix) a system of internal controls over changes to SCI systems;

(x) a plan for assessments of the functionality of SCI systems designed to detect systems compliance issues, including by responsible SCI personnel and by personnel familiar with applicable provisions of the Act and the rules and regulations thereunder and the SCI entity's rules and governing documents; and

(xi) a plan of coordination and communication between regulatory and other personnel of the SCI entity, including by responsible SCI personnel, regarding SCI systems design, changes, testing, and controls designed to detect and prevent systems compliance issues.

---

[24] In complying with this requirement, an SCI entity may wish to consider how closely its testing environment simulates its production environment; whether it uses appropriate development, acquisition, and testing controls; whether it identifies and corrects problems detected in the development and testing stages; whether it verifies change implementation in the production stage; whether development and test environments are segregated from SCI systems in production; and whether SCI entity personnel have adequately segregated roles between the development and/or test environment, and the production environment. *See* Adopting Release at 159.

[25] Rule 1001(a)(2)(v) holds any such plans for "critical SCI systems" to a higher standard than plans for resumption of trading operations more generally, requiring recovery for critical SCI systems within two hours. *See id.* at 170.

Additionally, SCI entities must periodically review the effectiveness of these policies and procedures and take prompt action to remedy any deficiencies in such policies and procedures. SCI entities should incorporate many of these requirements into their software development lifecycle protocols ("SDLC") and incident response policies and procedures. In the order settling the action against Knight Capital Americas LLC following that firm's trading incident in 2012,[26] the SEC similarly signaled that all broker-dealers should adopt and implement reasonably designed SDLC protocols and incident response policies and procedures pursuant to the Market Access Rule, Rule 15c3-5 under the Exchange Act. The Knight Capital order was not nearly as detailed as the explicit requirements of Reg SCI. Accordingly, broker-dealers should look to the above requirements for guidance regarding their SDLC and incident response policies and procedures.

B. Reasonably Designed Policies and Procedures

The required policies and procedures will be deemed to be "reasonably designed" if they are consistent with current SCI industry standards, "which shall be comprised of information technology practices that are widely available to information technology professionals in the financial sector and issued by an authoritative body that is a U.S. governmental entity or agency, association of U.S. governmental entities or agencies, or widely recognized organization."[27] The Proposing Release required that SCI entities comply with industry-standard information technology practices *available for free* and issued by the enumerated governmental agencies, associations or organizations. Upon deletion of that qualification on industry standards, SCI entities should now take into account all widely available industry practices, whether for free, for a fee or as part of a membership, issued by qualifying organizations. Compliance with such current SCI industry standards, however, is not the exclusive means to comply with the requirements of this section.

Simultaneous with Reg SCI's release, the SEC staff issued guidance regarding the standards for Reg SCI's required policies and procedures listed above.[28] In this guidance, the SEC staff sets forth certain approved standards related to systems capacity, integrity, resiliency, availability, and security; application controls; capacity planning; computer operations and production environment controls; contingency planning; information security and networking; audit; outsourcing; physical security; and systems development methodology. The SEC staff has listed what it views as standards by category meeting Rule 1001's requirements. The list includes

---

[26] *See Knight Capital Americas LLC*, Exchange Act Release No. 70694 at 8 (Oct. 16, 2013).

[27] Rule 1001(a)(4).

[28] *See* Staff Guidance on Current SCI Industry Standards, Securities Exchange Act Release No. 34-73639 (Nov. 19, 2014), *available at*: http://www.sec.gov/rules/final/2014/staff-guidance-current-sci-industry-standards.pdf.

standards issued by the National Institute of Standards and Technology; Federal Financial Institutions Examination Council; financial regulatory agencies including the SEC; the Institute of Internal Auditors; and the Security Benchmarks division of the Center for Internet Security.

This list includes standards approved, but not mandated, for subject entities' Reg SCI policies and procedures. That said, potential SCI entities should take note of these standards and assess their own systems, policies and procedures for compliance with these standards. By publicly issuing this guidance, the SEC staff has put the industry on notice that it will generally look for compliance and adherence to these standards by SCI entities. SCI entities should clearly document and justify any deviation from these standards in order to establish the reasonability of any such deviations. The SEC staff will expect, during an examination, to see this documentation and analysis comparing an SCI entity's systems, policies and procedures to these standards.

C. Corrective Actions Following an SCI Event

Reg SCI imposes duties upon SCI entities to take corrective action once any "responsible SCI personnel" has a "reasonable basis to conclude" that there has been an SCI event.[29] SCI entities, therefore, must mitigate potential harm to investors and market integrity as a result of the SCI event (described above), and devote "adequate" resources to remedy the event as soon as "reasonably practicable."[30] Responsible SCI personnel are senior managerial employees, and their designees, who have responsibility for a specific SCI system or indirect SCI system.[31]

The SEC, in the Proposing Release, initially suggested that responsible SCI personnel should take corrective action immediately upon "becoming aware of" an SCI event.[32] Crucially, the SEC changed this standard. As adopted, an SCI entity triggers the obligation to take corrective action when SCI personnel have "a reasonable basis to conclude" that an SCI event has occurred. While this is a seemingly lower standard, the SEC stated that this "reasonable-basis-to-conclude" standard affords responsible SCI personnel latitude to perform initial analyses, gather relevant information and assess whether there has been an SCI event before being required to take corrective action.[33] Responsible SCI personnel, however, cannot be willfully blind, and they must act in relation to an SCI event if they know, or should know, an SCI event has occurred. Junior employees and employees who

[29] Rule 1002(a).

[30] *Id.*

[31] *See* Rule 1000.

[32] *See* Adopting Release at 247.

[33] *See id.*

are not responsible for the affected system do not have an explicit duty to take corrective action or identify when an SCI event occurs. The policies and procedures, however, required by Rule 1001(a)(2)(vii), related to monitoring of SCI systems to identify potential SCI events, likely requires the adoption and implementation of policies and procedures for the reporting and escalation of systems issues by all employees.[34]

To satisfy Reg SCI, potential SCI entities should: (i) designate responsible SCI personnel for all SCI systems; (ii) adopt policies and procedures that provide for oversight by senior management of SCI systems; and (iii) and implement procedures that direct and identify means for junior employees to escalate potential systems issues to responsible SCI personnel. While responsible SCI personnel are permitted to appoint designees who are also responsible for particular SCI systems, they cannot disclaim responsibility through such designation.

D. Safe Harbor for SCI Entity Personnel

The Adopting Release makes clear that Reg SCI does not impose obligations directly on the personnel of SCI entities.[35] Moreover, Reg SCI provides a safe harbor from Reg SCI violations for individuals responsible for or having supervisory authority over SCI systems. The safe harbor applies to any "personnel of an SCI entity," which not only covers employees of SCI entities, but also contractors, consultants, and other non-employees.[36] An individual claiming the safe harbor, however, has the burden of proof with respect to the applicability of the safe harbor.[37] To qualify for the safe harbor, the individual must demonstrate that she: (i) satisfactorily performed her duties in accordance with the SCI entity's policies and procedures; and (ii) was without reasonable cause to believe that the Reg SCI-related policies and procedures were not established, maintained, or enforced in accordance with Rule 1001(b) in any material respect. The second prong applies only to personnel who have supervisory responsibility for SCI systems. Personnel without responsibility for an SCI system can qualify for the safe harbor regardless of their beliefs concerning whether the policies and procedures complied with Rule 1001(b), so long as they discharged their duties.[38]

---

[34] *See id.* at 178-180.

[35] *See id.* at 243.

[36] *See id.* at 233.

[37] *See id.* at 233.

[38] *See id.*

E. Reporting

In addition to requiring corrective action, Reg SCI imposes several reporting obligations upon SCI entities following the occurrence of an SCI event. Once responsible SCI personnel have a reasonable basis to conclude that an SCI event has occurred, the SCI entity must immediately notify the SEC of the SCI event.[39] Within 24 hours after concluding that an SCI event has occurred, the SCI entity must submit a written notification that, on a good faith, best efforts basis, provides: (i) a description of the SCI event; and (ii) identifies the system(s) affected.[40] Additionally, to the extent possible at the time of notification, the notification should include the SCI entity's assessment as to the extent of market participants affected, the SCI event's impact on the market, and information concerning the SCI entity's corrective actions.[41]

Thereafter, until the SCI event is resolved and the SCI entity's investigation into the event is closed, the SCI entity must provide ongoing updates to the SEC.[42] The updates, which do not need to be delivered in written form, should correct any materially incorrect information previously provided and provide material information discovered in the course of the investigation. An SCI event is deemed "resolved" when the event no longer meets the definition of an SCI event and the SCI entity has submitted its final report to the SEC regarding the SCI event.[43]

SCI entities are also required to provide further written notification by way of interim and final reports.[44] Once the SCI event is resolved and the SCI entity's investigation is closed, the SCI entity must submit a final written notification to the SEC. If an SCI event is not resolved within 30 days of its occurrence or the SCI entity's investigation is still ongoing, the SCI entity must submit an interim written notification.

---

[39] *See* Rule 1002(b)(1). This notification can be provided orally or in writing. *See* Adopting Release at 277.

[40] *See* Rule 1002(b)(2).

[41] *Id*.

[42] *See* Rule 1002(b)(3).

[43] *See* Adopting Release at 297-98.

[44] *See* Rule 1002(b)(4). Rule 1002(b)(4)(ii) requires the reports to include the following information: (i) "a detailed description of the SCI entity's assessment of the types and number of market participants affected by the SCI event; the SCI entity's assessment of the impact of the SCI event on the market; the steps the SCI entity has taken, is taking, or plans to take, with respect to the SCI event; the time the SCI event was resolved; the SCI entity's rule(s) and/or governing document(s), as applicable, that relate to the SCI event; and any other pertinent information known by the SCI entity about the SCI event"; (ii) "a copy of any information disseminated pursuant to [Rule 1002(c)] by the SCI entity to date regarding the SCI event to any of its members or participants"; and (iii) "an analysis of parties that may have experienced a loss, whether monetary or otherwise, due to the SCI event, the number of such parties, and an estimate of the aggregate amount of such loss." Importantly, Rule 1002(c) requires an SCI entity to disseminate information concerning the SCI event to its members or participants affected by the SCI event.

F. Periodic Reporting

In addition to the reports that must be filed after the occurrence of an SCI event, SCI entities are required to file several periodic reports. Pursuant to Rule 1002(b)(5)(ii), an SCI entity must submit quarterly reports of systems disruptions and systems intrusions which have had, or the SCI entity reasonably estimates would have, no impact or a *de minimis* impact on the SCI entity's operations or on market participants. Rule 1003(a)(1) requires an SCI entity to submit a quarterly report concerning all material changes to its SCI systems. Finally, an SCI entity must submit an annual report regarding the annual review of the entity's compliance with Reg SCI. This report must be submitted to senior management for review, and then must be sent together with responses by senior management to the SEC.[45] The report does not, however, need to be certified by senior management.[46]

G. Form SCI, Written Notifications, and FOIA

All written notifications and reports required to be submitted pursuant to Reg SCI must be filed electronically on Form SCI.[47] Because Form SCI is a report required to be filed under the Exchange Act, it is unlawful for any person to willfully or knowingly make, or cause to be made, a false or misleading statement with respect to any material fact in Form SCI.[48]

With regard to the initial written notification (within 24 hours) that must be provided to the SEC after an SCI event, the SEC explicitly recognizes that the information could be subject to FOIA requests.[49] Likewise, the interim and final reports addressing an SCI event would also likely be subject to FOIA requests. Though the SEC was silent on whether any specific FOIA exemptions could apply, 5 U.S.C. § 522(b) lists a number of possibly applicable exemptions from FOIA requests (*e.g.*, trade secrets, and otherwise privileged or confidential commercial or financial information).[50] The SEC also stated that, subject to the provisions of 17 C.F.R. § 200.80(b), it "generally will not publish or make available information contained in any reports, summaries, analyses, letters, or memoranda arising out of,

---

[45] *See* Rule 1003(b). The final report, with responses from senior management, is also sent to the SCI entity's board of directors or board equivalent.

[46] *See* Adopting Release at 362. This is in contrast, however, to the annual certification of compliance with Rule 15c3-5 that each registered broker-dealer must have completed by its CEO and file with the SEC. *See* 17 C.F.R. § 240.15c3-5(e) (2010).

[47] *See* Rule 1006. Form SCI provides specific prompts for short responses, as well as prompts for open-ended narrative responses.

[48] *See* Adopting Release at 416.

[49] *See id.* at 293.

[50] *See also* Freedom of Information Act Exemptions, *available at*: http://www.sec.gov/foia/nfoia.htm; The Department of Justice Guide to the Freedom of Information Act, *available at*: http://www.justice.gov/oip/doj-guide-freedom-information-act.

in anticipation of, or in connection with an examination or inspection of the books and records of any person or any other investigation."[51]

While it is possible that the reports and notifications required by Reg SCI may not be subject to FOIA requests, the SEC refused to guarantee this result. Until further guidance is issued, SCI entities should proceed with the understanding that any of the written reports provided to the SEC in response to an SCI event may be subject to a FOIA request.[52] This has clear civil litigation and discovery implications. Accordingly, SCI entities, and those that could become SCI entities, should carefully draft and implement policies and procedures related to SCI-event reporting. These policies and procedures should aim to satisfy the requirements of the rule, adhere to all relevant FOIA requirements (i.e., requesting confidentiality and satisfying any applicable exemption), protect the SCI entity from outside lawsuits (to the extent possible), and require the participation of the business, information technology, compliance and legal personnel in crafting the reports.

H. Recordkeeping

The Proposing Release would have required each SCI entity to provide the SEC with "reasonable access" to the SCI entity's SCI systems so that the SEC could assess the SCI entity's compliance with Reg SCI.[53] The SEC ultimately declined to adopt the "reasonable access" provision, choosing instead to implement and rely on robust recordkeeping requirements through Rule 1005 of Reg SCI.[54] Pursuant to Rule 1005, an SCI SRO must make, keep, and preserve all documents relating to its compliance with Reg SCI as prescribed in Rule 17a-1 under the Exchange Act. An SCI entity that is not an SCI SRO must:

- Make, keep, and preserve at least one copy of all documents relating to its compliance with Reg SCI, including, but not limited to, records relating to any changes to its SCI systems and indirect SCI systems;
- Keep all such documents for a period of not less than five years, the first two years in a place that is readily accessible to the SEC or its representatives for inspection and examination; and
- Upon request of the SEC or its staff, promptly furnish any documents required to be kept and preserved pursuant to Reg SCI.

---

[51] Adopting Release at 734.

[52] The annual report addressing the SCI entity's compliance with Reg SCI would also likely be subject to FOIA requests.

[53] *See id.* at 409.

[54] *See id.* at 412.

Rule 1005 of Reg SCI states that an SCI entity retains legal responsibility for systems operated on its behalf and, as such, is responsible for producing records to SEC representatives that are required to be made, kept, and preserved under Reg SCI, even if those records are maintained by third parties. The SCI entity is responsible for ensuring that any such third parties produce those requested documents, upon examination or other request. SCI entities should draft and, as necessary, amend their contracts with third parties to require compliance with this requirement. Moreover, to the extent that potentially subject entities, or their vendors, do not keep such records, SCI entities should conduct a full review of their recordkeeping practices related to their technological systems and implement new policies or procedures (and develop related systems and databases) necessary to comply with Reg SCI.

VI. CONCLUSION

Reg SCI imposes extensive new standards and procedural and reporting requirements on certain securities-related institutions, including national securities exchanges, ATSs that meet certain thresholds, plan processors, and exempt clearing agencies. Operators of ATSs should analyze their systems in light of Reg SCI and adopt and implement procedures to continuously monitor ATS activity in order to determine whether Reg SCI applies to their ATS now or in the future. Additionally, all entities subject to Reg SCI should evaluate their technological systems, and related policies and procedures, for compliance with the SEC's suggested standards for such systems, policies and procedures. Finally, Reg SCI includes extensive reporting requirements that raise issues related to confidentiality and litigation risk. Accordingly, all potentially subject entities should assess the applicability of Reg SCI and its reporting requirements and implement a related reporting program that satisfies the requirements of the regulation and protects the subject entity. Given the breadth of the regulation's requirements and specific focus on specified entities, any potentially subject entities should thoughtfully and carefully assess the regulation's applicability and requirements.

FINANCIAL INSTITUTIONS REGULATION GROUP

Please feel free to discuss any aspects of this Client Alert with your regular Milbank contacts or any of the members of our Financial Institutions Regulation Group.

If you would like copies of our other Client Alerts, please visit our website at www.milbank.com and choose "Client Alerts" under "News."

NEW YORK

One Chase Manhattan Plaza, New York, NY 10005

Wayne M. Aaron	waaron@milbank.com	+1-212-530-5284
Antonia M. Apps	aapps@milbank.com	+1-212-530-5357
George S. Canellos	gcanellos@milbank.com	+1-212-530-5792
Douglas Landy	dlandy@milbank.com	+1-212-530-5234
Richard Sharp	rsharp@milbank.com	+1-212-530-5209
Aaron Renenger	arenenger@milbank.com	+1-212-835-7505
John Williams	jwilliams@milbank.com	+1-212-530-5537
Dorothy Heyl	dheyl@milbank.com	+1-212-530-5088
Tamika Bent	tbent@milbank.com	+1-212-530-5547
Julia Hueckel	jhueckel@milbank.com	+1-212-530-5539
John Yarwood	jyarwood@milbank.com	+1-212-530-5369